IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSASCHUSETTS

CHESTNUT DENTAL ASSOCIATES, P.C.

Plaintiff,

v.

SOVEREIGN BANK, N.A.

Defendant.

CIVIL ACTION NO. 1:12-_____

**COMPLAINT AND JURY DEMAND**

Plaintiff, Chestnut Dental Associates, P.C., by its undersigned counsel, states the following as its Complaint against Defendant Sovereign Bank, N.A.

**PRELIMINARY STATEMENT**

This action arises out of Sovereign Bank's failure to fulfill one of its most basic obligations, namely, to protect its customers' funds against theft. From June 25, 2012 through approximately July 10, 2012, cybercriminals accessed Chestnut Dental Associates' accounts at Sovereign Bank and wire transferred over two hundred twenty-two thousand dollars to accounts at several banks, including accounts in Hong Kong and Malaysia. After Sovereign Bank provided the cybercriminals with its customers complete account numbers and balances, the Bank failed to follow its own security procedures for wire transfers, failed to follow reasonable security procedures whatsoever, and failed to identify out of the ordinary transfers despite a banking relationship of over forty years without any international wires. Further, the Bank failed to identify obvious fraud in the completion of wire transfer requests and even assisted the cybercriminals in correcting the deficiencies. Sovereign Bank allowed the cybercriminals to wire the customer's funds from the customer's operating account, which had only been used for a single annual December wire funds from its operating account to its payroll company's

(ADP) account. Despite the Bank's dramatic failure to protect its customer's money, the Bank, adding insult to injury has unfairly demanded that the customer be responsible for the loss. Chestnut Dental Associates has requested that the Bank restore its account balance, based upon the Bank's failures recited herein and the recent First Circuit of the United States Court of Appeals decision in Patco Construction Company, Inc. v. People's United Bank, d/b/a Ocean Bank, 684 F.3d 197, United States Court of Appeals, First Circuit (July 3, 2012).

## THE PARTIES

1. Plaintiff, Chestnut Dental Associates, P.C. ("CDA") is a Massachusetts Corporation with a principal place of business in Needham, Massachusetts.
2. Sovereign Bank, N.A. ("Sovereign" or the "Bank") is a wholly owned subsidiary of Banco Santander, S.A., a Virginia Corporation and with a business location at 75 State Street, Boston, Massachusetts.

## JURISDICTION AND VENUE

3. This action is of a civil nature involving, exclusive of interest and costs, a sum in excess of $75,000. Every issue of law and fact is wholly between citizens of different states.
4. This Court has subject matter jurisdiction pursuant to 28 U.S.C.A. § 1332.
5. This Court has personal jurisdiction over Defendant pursuant to Massachusetts G.L. c. 223A, Section 3(a) (the "Massachusetts Long-Arm Statute").
6. Venue is proper in this Court pursuant to 28 U.S.C.A. § 1391(2) as the tortious act complained of was committed in Massachusetts.

## THE FACTS

7. CDA has been in business since 1970, and incorporated as a Professional Corporation pursuant to Massachusetts law in 1980. CDA is a regional dental practice, providing pediatric, orthodontic and general dentistry to the communities surrounding Needham and Franklin, Massachusetts.
8. CDA has banked with Sovereign, or its predecessors, since its formation.
9. CDA maintains an operating account (hereinafter, the "account" or "CDA account") and other deposit, payroll and loan accounts as a business banking customer of Sovereign.
10. CDA uses ADP as its payroll service provider to pay its partners and employees.
11. For at least the last fifteen years, CDA would include an additional December payroll to pay partner and/or employee bonuses (the "December Bonus Payroll").
12. CDA's payroll company required CDA to wire transfer funds to the payroll company's account for this December Bonus Payroll, if the amount of the payroll exceeded a pre-determined amount, which had in fact occurred over the past several years, except in 2011.
13. Specifically to accommodate the payroll company's wire transfer requirements for the December Bonus Payroll, CDA requested that Sovereign permit CDA the ability to wire transfer funds from its operating account.
14. In its past 40 years as a customer of Sovereign, CDA's only wire transfers were for the December Bonus Payroll.

15. To complete the December Bonus Payroll, CDA would meet with its accountant at CDA's offices to complete the wire transfer request form and fax the form to the Bank.
16. For example, in 2010, the December Bonus Payroll was completed by CDA by sending a completed form (the "2010 Wire Transfer Agreement") by fax from CDA to Sovereign.
17. The 2010 Wire Transfer Agreement was completed and then signed by Jonathan Chason.
18. The 2010 Wire Transfer Agreement provided the correct name and address of the customer.
19. The 2010 Wire Transfer Agreement provided the correct account number.
20. The 2010 Wire Transfer Agreement required a phone call from Sovereign to Jonathan Chason, D.M.D. at the CDA office to verify the identity of the transferor and confirm that the account holder had requested the transfer
21. On information and belief, Sovereign required telephone verification by Jonathan Chason, D.M.D. a shareholder in CDA or, more recently, Jack Hertzberg, D.M.D, a shareholder in CDA.
22. In its 40 year banking relationship with Sovereign, CDA never wire transferred funds to vendors, suppliers or any party, other than its payroll company for the December Bonus Payroll.
23. During its 40 year existence and banking relationship with Sovereign, CDA would be serviced by a Sovereign employee for loans and account questions.

24. For the past several years, Scott Vickery, Vice President, Business Banking Relationship Manager was the Sovereign employee assigned to the CDA account.
25. Historically, CDA would borrow money from Sovereign for major equipment purchases, such as evidenced by its UCC filing of August 8, 2003 with the Massachusetts Secretary of State, Corporations Division.
26. CDA had previously worked with Scott Vickery on its active equipment loans with Sovereign.
27. For its existing equipment loans, CDA did not purchase the collateralized equipment from manufacturers, but rather, from major United States based dental distributors, who could deliver, install, service, maintain and provide disposables for the equipment.
28. When CDA applied for collateralized equipment loans, CDA ultimately submitted invoices for its proposed equipment purchases to Sovereign.
29. In connection with its collateralized equipment loans, CDA did not provide the Bank with evidence of any international equipment purchases, but rather, equipment provided by regional dental equipment distributors.
30. CDA understood the wire transfer process to require Jonathan Chason, D.M.D.'s or Jack Hetzberg, D.M.D.'s verbal approval by confirmatory telephone call from the bank to CDA's office.
31. Sovereign did not offer CDA any fax wire transfer authentication that would provide multi-layered authentication.

32. Sovereign did not offer to CDA, both the ability to block transfer requests from emails or during times other than its customary late December Bonus Payroll wire transfer.

**The 2012 equipment and buildout loan**

33. On or about May 2012, CDA applied for an equipment and buildout loan from Sovereign (the "2012 equipment and buildout loan").

34. Dr. Jack Hertzberg ("Dr. Hertzberg") is a partner of CDA.

35. On or about May 17, 2012, in contemplation of a potential new equipment loan between CDA and the Bank, Dr. Hertzberg corresponded with Scott about unfreezing Dr. Hertzberg's credit report, so that the Bank could obtain a copy for the loan application process.

36. In accordance with its prior practices in applying for equipment and buildout loans, Sovereign required a proposed budget and equipment expense detail for the loan application for the 2012 equipment and buildout loan.

37. On June 4, 2012, at 9:21 a.m., Jonathan Chason, D.M.D. ("Dr. Chason"), a shareholder of CDA, who was coordinating renovations to CDA's Franklin, Massachusetts office, sent a cost breakdown to Scott (the "June 4, 2012 budget").

38. The June 4, 2012 budget provided for a total expense of $70,825.

39. The June 4, 2012 budget provided for an estimated $33,825 in total "Operatory and related mechanical room" expense.

40. On June 5, 2012 at 5:24 p.m., Peter McNicholas, Administrator for CDA, sent Scott Vickery, Vice President, Business Banking Relationship Manager at

Sovereign Bank ("Scott") an email containing the proposed budget for the 2012 equipment and buildout loan also in the amount of $70,825.

41. In his June 5, 2012 5:24 p.m., email to Scott, Peter McNicholas included a "quote from our equipment vendor relative to the Franklin Office renovation we plan on starting in August, 2012."

42. The equipment quote sent to Scott in the June 5, 2012 email was dated April 2, 2012 and was prepared by Henry Schein Dental, of Needham, Massachusetts (the "Equipment Quote").

43. The Equipment Quote totaled $36,946.10 and was addressed to the attention of Dr. Debra Blattman of CDA.

**The infiltration of CDA's Account at Sovereign**

44. Based upon information and belief, at some point on or before June 5, 2012, Dr. Hertzberg's gmail account was hacked into by a perpetrator ("Fake Jack" or the "cybercriminal(s)").

45. Apparently, Fake Jack was able to monitor Dr. Hertzberg's email correspondence and picked up on some correspondence between Dr. Hertzberg and Scott.

46. On Tuesday, June 5, 2012 at 8:47 a.m., Fake Jack emailed Scott, stating the following:

> "Hi,
> Could you please provide me all my account balances?"

47. On Tuesday, June 5, 2012 at 8:48 p.m., Scott replied to the e-mail requesting account balances by stating the following:

> "Are you looking for Sovereign Bank account balances for Chestnut Dental? For you personally?
>
> Is everything ok?
>
> Thanks"

48. Dr. Hertzberg had never requested account balances for CDA from Scott or anyone else at Sovereign for CDA accounts prior to June 5, 2012.

49. Dr. Hertzberg had never requested that Scott help him in accomplishing a wire transfer of funds.

50. On June 5, 2012 at 8:54 a.m., Fake Jack emailed Scott, stating the following:

> "Provide me all, Everything is fine.
>
> Thanks"

51. On June 5, 2012 at 9:23 a.m., without first attempting to telephone Dr. Hertzberg to verify his identity and request, Scott emailed Fake Jack all of CDA's COMPLETE account numbers and balances for deposit and loan accounts.

52. On information and belief, sending a customer's account numbers and balances by unsecured email violated Sovereign's policies and procedures.

53. Dr. Hertzberg was unaware that his account was hacked or that communication between the Bank and Fake Jack had occurred.

54. On Tuesday, June 5, 2012 at 9:27 AM, Fake Jack emailed Scott stating:

> "Thanks for your prompt response,
>
> Actually, I'm buying some Xray machines and Orthodontic equipments from a company in Malaysia and would probably need you make a wire transfer to them. What recipient details is required?
>
> Thanks"

55. Despite the grammatical errors in the June 5th 9:27 a.m. email purported to be from Dr. Hertzberg, Scott did not attempt to verify the identity of the sender.

56. Instead, shortly thereafter on June 5, 2012, at 11:14 a.m., Scott emailed Fake Jack the information required to complete a wire transfer from the Bank, including the recipient details the Bank would need to process the wire.

57. In the June 5, 2012 11:14 a.m. email, Scott also stated:

> "…Any concern with the seller? Do you want to speak with someone from our international trade group to discuss potential ways to protect yourself?"

58. Seven minutes later, on June 5, 2012 at 11:21 a.m., Fake Jack replied to Scott, as follows:

> "No concern with the seller as I have tested and verified them earlier before now. I just concluded with them and the total cost of the equipments is of 31,360usd. Below is the recipient details provided.
>
> Beneficiary Name: LShadow Inc Ent
> Beneficiary Account No:--------
> Bank Name: Public Bank
> Bank Address:…Malaysia
> Swift Code:----
>
> Will this do?
>
> Send me the reference slip once done.
>
> Thank you."

59. Despite the grammatical errors in yet another email purported to be from Dr. Hertzberg, and the unusual reference to "usd" and declination of opportunity to "protect" himself in the international transaction, from an individual who maintained a "freeze" on his personal credit account, Scott again did not attempt to verify the identity of the sender.

60. On Tuesday, June 5, 2012 at 11:26 AM, Scott emailed Valerie Tipton of Sovereign ("Valerie") requesting,

> "Can you initiate a one time wire? Or **do I need to send him to the branch**."{*emphasis supplied}.

61. On information and belief, Sovereign Bank's policies and procedures for this international wire transfer required the customer to be identified at the Bank branch.

62. On information and belief, Sovereign Bank's policies and procedures for this international wire transfer required a call back to the registered phone number of the customer maintained by the Bank.

63. On Tuesday, June 5, 2012 at 11:30 AM, Valerie emailed Scott stating,

> "Hi Scott: I can do this wire, but the customer needs to put all info on the official form. The wire is over $10M, so we will need to do a callback to the signer to go over all information the form.
> Need beneficiary address…no PO Boxes.
>
> It is attached.
>
> Thanks, Val."

64. On Tuesday, June 5, 2012 at 11:34 AM, Scott emailed Fake Jack and wrote:

> "Hi Jack
>
> Val needs the attached form completed, signed and faxed back. See her email and fax number below.
>
> Thanks"

65. On June 5, 2012 5:24 p.m., Scott received Peter McNicholas' email which included the Equipment Quote, relative to the Franklin Office renovation, prepared by Henry Schein Dental, of Needham, Massachusetts.

66. Scott did not attempt to address the inconsistency in the purported vendors.

67. Scott did not attempt to address the inconsistency in the budgeted amounts.

68. Scott did not attempt to contact Dr. Chason about the changes.

69. On Monday, June 25, 2012 at 8:26 AM, Fake Jack emailed Scott, stating:

> "OK, I asked you to help me make a transfer for some equipments earlier. I attached the completed wire transfer form below. Can you process it today and send me the reference slip. Thanks Jack"

70. Scott did not question the grammatical, punctuation or other signs of the cybercriminal in the June 25, 2012, 8:26 a.m. email from Fake Jack.

71. On June 25, 2012, at 8:29 a.m., Scott sent the fraudulently completed wire transfer form to Valerie, which was inconsistent with the "fax" delivery method previously required by the Bank.

72. On Monday, June 25, 2012 at 8:57 a.m., Scott emailed Fake Jack, stating,

> "Thanks Jack
> I will ask Val and Helen to process. They will need to contact you to verify the info by phone as the amount is over $10K. What's the best number to reach you?
>
> Also, the account number on the form is one of your loan #s. Can you either correct the form or verify the checking account number in an email? I cc'd Peter in case you don't have the number handy.
>
> Sorry for the inconvenience
> Thanks"

73. The fraudulent June 25, 2012 wire transfer agreement was not in the name of the account holder.

74. The fraudulent June 25, 2012 wire transfer agreement contained an incorrect account holder address.

75. The fraudulent June 25, 2012 wire transfer agreement listed the prior residential address of Dr. Hertzberg, although he had not resided at the address for over twelve years.
76. The fraudulent June 25, 2012 wire transfer agreement did not contain the operating account number, but rather the account holder's loan account number.
77. The fraudulent June 25, 2012 wire transfer agreement was not signed by anyone.
78. The fraudulent June 25, 2012 wire transfer agreement did not contain the tax identification number of the account holder.
79. Upon learning of the incorrect "loan" account number and discrepancies on the transfer request form, Scott did not call Dr. Hertzberg on his cell phone, which number was readily available in the email chain, to verify that Dr. Hertzberg initiated the request.
80. Upon learning of the incorrect "loan" account number and discrepancies on the transfer request form, Scott did not call Dr. Chason, Peter McNicholas or CDA's office phone, which numbers were readily available, to verify that Dr. Hertzberg initiated the request.
81. Instead, Scott requested that the cybercriminal provide a phone number for verification.
82. The cybercriminal provided Scott with a phone number which was not associated with anyone at CDA or Dr. Hertzberg.
83. On information and belief, on Monday, June 25, 2012, Scott emailed Fake Jack informing him that the account number in the Wire Transfer Agreement was a loan number and Scott asked the Fake Jack to resubmit a correct form or verify,

via email, the checking number, and stated that he copied Peter McNicholas, Administrator of CDA, in case Fake Jack did not have the number handy.

84. On Monday, June 25, 2012 at 9:04 a.m., Fake Jack responded to Scott that:

> "I'm quite busy now and won't be able to pick calls now until I'm done. The Checking Account # is 8XXXXXXXX. Please process it and send me the reference number. I'll give you a call when im done
> Thanks Jack"

85. On Monday, June 25, 2012 at 9:09 a.m., Scott responded to Fake Jack:

> "Jack
> Someone on the account needs to verify the wire info with the relationship assistant before they can process the wire as this in not being processed in person at a branch. This is a required step that they cannot avoid.
> I'm sorry for the inconvenience.
> Thanks"

86. On Monday, June 25, 2012 at 9:17 a.m., Fake Jack provided a phone number to Scott which was 817-381-5710 (the "cybercriminal's phone number"), which was not a phone number listed on CDA's account, associated with Dr. Hertzberg, and, on information and belief, the "817" area code is a Texas area code.

87. Scott had personally spoken with Dr. Hertzberg on many occasions on Dr. Hertzberg's cell phone, home phone or office numbers only and they were familiar with each other's voice and some personal history.

88. On information and belief, Scott did not call the cybercriminal's phone number to confirm identity, but rather, provided "Helen Chang" of Sovereign, who had never spoken with Dr. Hertzberg, with the cybercriminal's phone number.

89. On Monday, June 25, 2012 at 9:18 a.m., Scott emailed Fake Jack stating that Helen would call him shortly.

90. On information and belief, at some time after 9:18 a.m., Helen dialed the phone number provided by Fake Jack and spoke with someone.

91. On information and belief, at some time after 9:18 a.m., after speaking with someone answering the perpetrator's phone, Helen requested further identification from Fake Jack.

92. On Monday, June 25, 2012 at 10:29 a.m., Fake Jack provided, in an unsecure email to Scott and Helen, a pilfered copy of Dr. Hertzberg's passport as identification, and stated:

> "Attached is the form and a copy of my ID(Passport) requested. I hope you can process today. Send me the reference details. Thanks Jack"

93. Dr. Hertzberg, upon advice obtained from a travel related source, had stored a copy of his passport in an email folder, which the cybercriminals were able to obtain.

94. On Monday, June 25 at 10:31 a.m., Scott emailed Fake Jack to confirm the wire was transferred and provided him with the federal identification confirmation number.

95. On June 25, 2012, Sovereign sent an international wire transfer from CDA's account to Malaysia in the amount of $31,360.

96. On June 26, 2012, at 8:03 a.m., Fake Jack emailed Scott, stating:

> "When'll the recipient receive the payment? Could you possible send mea soft copy of the confirmation slip as the recipient requested for it. Thanks Jack"

97. On June 26, 2012 at 8:17 a.m., Scott emailed Fake Jack and Valerie, stating in part, that, "…I suspect they could have funds today…"

98. On information and belief, on Tuesday, June 26, 2012 at 8:27 a.m., after intercepting and reading an email to Fake Jack concerning a wire transfer, prior to Fake Jack deleting the email, Dr. Hertzberg emailed Peter McNicholas asking if Peter McNicholas asked for a wire transfer as Dr. Hertzberg had not done so.

99. On Tuesday, June 26, 2012 at 8:30 a.m., Valerie emailed Scott informing him that "[i]nternational wires can take up to a week to arrive at their destination…."

100. On Tuesday, June 26, 2012 at 8:35 a.m., Peter McNicholas emailed Dr. Hertzberg asking for Dr. Hertzberg to call him and stating that he did not request a wire transfer.

101. On Tuesday, June 26, 2012 at 8:44 a.m., Fake Jack emailed Scott requesting a second wire, stating:

> "OK, I actually will still need you to help me send another wire transfer of 8K euros to Germany. I'll fill the form and let you know before the end of the day. Thanks Jack."

102. On Tuesday, June 26, 2012 at 8:48 a.m., Fake Jack emailed Peter stating that "I mean, I already corrected it. Thanks"

103. On Tuesday, June 26, 2012 at 8:52 a.m., Peter McNicholas emailed Scott stating:

> "Scott, Good morning. I just spoke with Dr. Hertzberg, as I was confused about the request for a wire transfer I saw in an email. Call my cell if you can to review. My cell is 878-201-1086, Thanks, Peter."

104. On Tuesday, June 26, 2012 at 9:07 a.m., Scott emailed Fake Jack and Peter and stated:

> "Hi Jack

> We don't have a slip. The confirmation number we sent you is typically all that is provided. Nevertheless, I will try to put something together for you.
> Val indicated that international wires can take up to a week depending on the country."

105. On Tuesday, June 26, 2012 at 9:10 a.m., Scott emailed Fake Jack and stated:

> "OK
> Is this also coming out of the Chestnut account? Please make sure that the account name and checking account # match of the form.
> Thanks"

106. On Tuesday, June 26, 2012 at 9:12 a.m., Scott emailed Peter McNicholas that the number was not working.

107. As Peter McNicholas mistakenly gave Scott the wrong phone number, with the first number of the area code mistakenly typed as an "8" instead of a "9", Peter corrected the number at 9:15 a.m.

108. On Tuesday, June 26, 2012 at 9:18 a.m., Scott called Peter on his cell phone.

109. On Tuesday, June 26 at 9:18 a.m., Peter McNicholas received a phone call from Scott's cell phone (508-308-1209) during which Peter McNicholas recalls telling Scott that no one at CDA had authorized the wires and Scott responding that he would take care of this.

110. On information and belief, after the phone conference with Peter McNicholas, the cybercriminal communicated by email with Scott about the wire transfer.

111. On Tuesday, June 26, 2012 at 9:28 a.m., Scott emailed Fake Jack indicating that he would receive an e-mail confirmation with the wire detail.

112. On Tuesday, June 26 at 9:50 a.m., an email was sent from pmnicho4@gmail.com posing as Peter McNicholas (the "Fake Peter") to Dr. Hertzberg stating

> "Also Talked to Scott Vickery. He said it was a mistake and we've settled it. He said you should ignore the message. Peter."

113. Peter McNicholas's actual email account is pmnich4@gmail.com.

114. On Tuesday, June 26, 2012 at 10:56 a.m., Fake Jack emailed the second Wire Transfer Agreement form and reconfirmed the account details for the transfer. They were as follows:

> "Account Holder: Frank Mottulla, Weserberghausweg 3a, 31737 Rintein Germany. Bank: Sparkasse Schaumburg, IBAN: DE91 XXXXXXXXXXXX, Swift-XXXXXXXXXXX, Amount: 8,000 euros"

115. On Tuesday, June 26, 2012 at 11:25 a.m., Scott emailed a reply to Fake Jack, stating

> "Hi Jack
>
> The account name and address needs to match the account number. You listed your personal name and address. I assume this is for Chestnut Dental. I am not allowed to change otherwise I'd make the change for you. If its for Chestnut Dental, can you change the name and address please?
> I know they processed the one yesterday, but they cannot process a second one with incorrect info. Once we have the corrected form we will send for processing. The wire department will then forward a confirmation email. Not sure if that is same day or next day. Wires after 2pm go out next day.
> I appreciate it
> Thanks"

116. On June 26, 2012, Fake Jack replied only to Scott, attaching the fraudulent wire transfer form.

117. Sovereign initiated international wire transfer to Germany of $10,492 on June 26, 2012.

118. The fraudulent June 26, 2012 wire transfer agreement was not in the name of the account holder.

119. The fraudulent June 26, 2012 wire transfer agreement contained an incorrect account holder address.

120. The fraudulent June 26, 2012 wire transfer agreement listed the prior residential address of Dr. Hertzberg, although he had not resided at the address for over twelve years.

121. On Monday, July 2, 2012 at 2:09 p.m., Fake Jack emailed Scott, stating:

> "Hi Val, I contacted Scott Vickery but he seems to be out of office. I'd probably need you to help me wire the rest for the equipments tomorrow. I'll complete the wire transfer form and send you once I conclude with the recipient. I hope you can help me get it done tomorrow morning. Thanks Jack."

122. On Tuesday, July 3, 2012 at 2:12 a.m. (date stamped "p.m.", but appears to actually be "a.m."), Valerie replied to Fake Jack stating:

> "Hello Jack: I can help you with the wire tomorrow.
> In the meantime, did you receive the e-mails from Scott and myself regarding the existing wire to Malaysia? More information is needed by the beneficiary bank."

123. On Tuesday, July 3, 2012 at 8:22 a.m., Fake Jack replied to Valerie stating:

> "Good morning Val, The recipient for the wire transfer in Malaysia has not yet received the payment. What is going on? Did you sent the recipient bank the additional details they requested yet? Thanks Jack

124. On Tuesday, July 3, 2012 at 8:30 a.m. (date stamped "p.m.", but appears to actually be "a.m."), Valerie responded to Fake Jack that:

> "The recipient bank needs more detail and that detail has to come from **you**.

> You need to send me the written wire instructions you received from the beneficiary. Once we look at that, you may need to contact the beneficiary for additional information.
> We do not contact the beneficiary for information.
> Valerie."

125. On Tuesday, July 3, 2012 at 8:41 a.m., Fake Jack replied to Valerie that:

> "I actually don't understand what other information you need but I will contact the beneficiary and let you know before the end of the day. I will send you the completed wire transfer form so that you can help me complete the other transfer for the rest of the equipments from Hong Kong. Thanks Jack."

126. On Tuesday, July 3, 2012 at 8:42 a.m. (date stamped "p.m.", but appears to actually be "a.m."), Valerie emailed Fake Jack and said

> "Jack: I need to see the wire instructions the beneficiary gave you. He must have sent you something in writing…"

127. On Tuesday, July 3, 2012 at 10:55 a.m., Fake Jack responded to Valerie, stating:

> "The invoice i sent you earlier is the instruction the recipient gave. Will that do?. Jack"

128. On Tuesday, July 3, 2012 at 11:10 a.m. (date stamped "p.m.", but appears to actually be "a.m."), Valerie emailed Fake Jack and said

> "Please send information to me as it was given to you by beneficiary. Did they give you an invoice?"

129. On Tuesday, July 3, 2012 at 11:19 a.m., Fake Jack responded and said:

> "I have forwarded you the invoice in a separate email. Did you get it? Jack"

130. On Tuesday, July 3, 2012 at 11:25 a.m., Valerie responded:

> "Yes. I have sent it to our wire processing area and they will try to figure out what is needed. Valerie"

131. On Tuesday, July 3, 2012 at 11:29 a.m., Fake Jack replied to Valerie:

> "Ok, Will you still be able to help me send the wire transfer for the remaining equipments to the other supplier today?"

132. On Tuesday, July 3, 2012 at 11:32 a.m., Valerie wrote:

> "Yes. Please complete the form and e-mail it to me. Please be available for a call-back/verification if the wire is over $10,000. Valerie"

133. For the July 3, 2012 wire transfer request, Sovereign again did not require the wire transfer agreement to be faxed.

134. On Tuesday, July 3, 2012 at 12:01 p.m., Fake Jack emailed a fraudulent wire transfer agreement to Valerie and provided the same fraudulent phone number for a call-back, stating:

> "Attached is the completed form. Call me. 817-381-5710. Thanks Jack"

135. On Tuesday, July 3, 2012 at 12:49 p.m., Fake Jack emailed Valerie, stating:

> "Send me the reference details when done. Thanks Jack"

136. On Tuesday, July 3, 2012 at 1:16 p.m. (date and time of email stamp appears incorrect), Valerie emailed Fake Jack confirmation of the wire and the reference number.

137. On July 3, 2:01 p.m., Fake Jack emailed Valerie stating:

> "The name is Mundo Bekti Dunia Company and not Mundo Berti Dunia Company. Could you please correct that? It is very important. Thanks Jack."

138. On July 3, 2:24 p.m., Fake Jack emailed Valerie stating:

> "OK, Val. How long will it take both recipient(Malaysia and HK) to receive the payment? Thanks Jack."

139. On July 3, 2012, Sovereign sent an international wire transfer to Hong Kong from CDA's account in the amount of $85,060.

140. The July 3, 2012 wire transfer agreement for the Hong Kong transfer was in the name of the account holder, but still had the fraudulent phone number.

141. Sovereign did not verify the identification of the purported transferor by call back to the account holder's office.

142. Sovereign did not verify the identification of the purported transferor by requiring its approved account holder to show identification at Sovereign's office.

143. On Friday, July 6, 2012 at 8:52 a.m., Fake Jack emailed Valerie, stating:

> "Good morning Val, I received mail from the recipient Malaysia, The recipient account has not yet been credited. What's happening? The transfer has been done since last month. Please check and let me know what's going on. Thanks Jack"

144. On Friday, July 6, 2012 at 11:24 a.m., Valerie emailed Fake Jack stating:

> "The wire room has sent an amendment (address correction) to the original wire. They will let me know when a reply is received. Our wire area, corrected the beneficiary address. What you had on your wire form for an address and what was on the invoice did not match. Val."

145. Sovereign failed to call its customer's office upon discovering the discrepancy in the transfer form and purported invoice.

146. On Monday, July 9, 2012 at 8:31 a.m., Fake Jack emailed Valerie and Scott, stating:

> "Good morning, I received message from both recipient. Both recipient haven't received the payments yet. Whats going on? Could you send a tracer dso that we can know the status of both transaction? Thanks"

147. On Monday, July 9, 2012 at 8:39 a.m. (date stamped "p.m.", but appears to actually be "a.m."),Valerie replied to Fake Jack, stating:

> "Hello Jack: As I emailed you on Friday, the correction to the wire to Malaysia has been sent. We are waiting for the beneficiary bank to receive our correction and process the wire. Even though it was sent on Friday, due to the time difference, they may not have received it until Saturday.
> The wire we sent on Tuesday, the 3rd, can take up to 5 days to reach its destination. Valerie"

148. On Monday, July 9, 2012 at 8:44 a.m., Fake Jack emailed Valerie, stating:

> "OK, I need you to help me make a local transfer of 10k to The Bancorp Bank this morning. How long will that take? Do i have to fill the same wire transfer form? Thanks Jack"

149. On Monday, July 9, 2012 at 8:45 a.m. (date stamped "p.m.", but appears to actually be "a.m."), Valerie emailed Fake Jack, as follows:

> "Yes, same form. A call back will be needed. Valerie"

150. On Monday, July 9, 2012 at 8:48 a.m., Fake Jack emailed Valerie, stating:

> "OK. How long does local transfers take?"

151. On Monday, July 9, 2012 at 8:49 a.m. (date stamped "p.m.", but appears to actually be "a.m."), Valerie emailed Fake Jack and informed him that domestic wires were usually processed same day.

152. On Monday, July 9, 2012 at 9:43 a.m., Fake Jack emailed Valerie yet another fraudulent wire transfer agreement, stating "Attached is the completed form and I reconfirm the details below."

153. On The Wire Transfer Agreements provided to Sovereign by Fake Jack contained a fraudulent phone number, which did not match any number that the Bank would have had on file for CDA or Dr. Hertzberg.

154. On Monday, July 9, 2012 at 10:23 a.m., Valerie emailed Fake Jack confirmation of the transfer request made that day.

155. On Monday, July 9, 2012 at 10:27 a.m., Fake Jack emailed Valerie, requesting:

> "Ok, Provide me all my account balances, Thanks."

156. On Monday, July 9, 2012 at 10:32 a.m., Valerie replied, copying Scott, as follows:

> "Jack: Please provide the last 4 digits of the accounts you want balances for."

157. On July 9, 2012 at 10:39 a.m., Fake Jack requested that Valerie provide him with account balances from a money market account and two checking accounts.

158. On Monday, July 9, 2012 at 10:51 a.m., Scott emailed Fake Jack, stating as follows:

> "Jack,
> Will you need additional wires?
> Val has been processing them for you but if you will need to send wires routinely we should set you up with either online wire function or have a pin pack sent so you can call them into our wire room directly. Thanks"

159. On Monday, July 9, 2012 at 11:40 a.m., Valerie emailed Fake Jack, copying Scott, and informed him that there were six figure balances in two of the requested accounts and zero in the other.

160. On July 10, 2012, Sovereign transmitted an international wire transfer to Malaysia in the amount of $95,310 from CDA's account.

161. On The Wire Transfer Agreements provided to Sovereign by Fake Jack contained a fraudulent phone number, which did not match any number that the Bank would have had on file for CDA or Dr. Hertzberg.

162. None of the fraudulent wire transfers were approved by a reasonable security procedure, such as a Bank call to Jonathan Chason, D.M.D. or Jack Hertzberg, D.M.D. at the CDA office phone number associated with the account.

163. Dr. Herzberg is one of nine shareholder's in CDA.

164. No other shareholder was contacted by the Bank about these wire transfers.

165. The Wire Transfer Agreements for each of the wire transfers sent by Fake Jack to Scott contained a fraudulent phone number, not associated with any CDA or Jack Hertzberg account.

166. On information and belief, the Bank never called any of the phone numbers listed on CDA's account to verbally confirm the wire transfer requests.

167. On information and belief, the Bank never faxed a wire confirmation to CDA's on file fax number.

168. On or about July 11, 2012, CDA discovered the fraud upon learning of its cash balance, and further investigating the discrepancy from its quickbooks balance and discovering the multiple wires.

169. Peter McNicholas then called Scott Vickery about the discovery.

170. Upon learning of the theft, CDA completed a loss affidavit, contacted the local police department to report the theft and demanded that its account balance be restored by the Bank.

171. In her August 21, 2012 letter to Jay Pabian, CDA's corporate attorney, Sovereign General Counsel Denise Goudet, Esq. ("Denise") wrote, "the bank did attempt a call-back to confirm these wires. Unfortunately, the telephone number

used for the call-back was not a valid telephone number of Chestnut Dental Associates, P.C."

172. Despite the wire transfer form indicating an incorrect contact number, the Bank proceeded with the wire transfer requests.

173. The first two Wire Transfer Agreements listed Dr. Hertzberg personally as the customer and not CDA.

174. The first two Wire Transfer Agreements listed a personal mailing address for Dr. Hertzberg that he had not resided at for over 12 years.

175. On information and belief, during the fraud, Scott advised Fake Jack on correcting errors on the Wire Transfer Agreements.

176. Ms. Valerie Tipton ("Valerie"), an employee of Sovereign Bank, also struggled with obtaining the proper information from Fake Jack on numerous occasions.

177. In the only known phone conversation between CDA and the Bank concerning wire transfer requests, on June 26, 2012, Peter McNicholas, CDA's Administrator, told Scott that no one at CDA had authorized the wires and Scott responded that he would take care of this.

178. Nevertheless, the Bank processed two additional international wires on July 3, 2012 and July 10, 2012.

179. On information and belief, the Bank did not provide any written wire transfer confirmations to CDA.

180. On information and belief, all confirmations went to Fake Jack via email correspondence.

181. As of August 3, 2012, $31,310 from the first wire of June 25, 2012 has been returned to CDA and $10,106.09 from the second wire on June 26, 2012 has been returned to CDA.

182. Sovereign indicated during the week of August 7, 2012, that it was highly unlikely that any additional monies could be recovered from the perpetrators.

183. Sovereign has denied CDA's request for a copy of the Bank's policies and procedures for initiation, verification and processing of wire transfers.

184. Sovereign has denied CDA's request for a copy of other emails sent to the Bank from the cybercriminal(s) related to these fraudulent wire transfers.

185. Sovereign knew or should have known that the authentication procedures used was known to be lacking in any reasonable fortification against attacks on customer accounts.

186. Sovereign, despite the widespread information and knowledge on phishing attacks and the need to adopt, educate and utilize sufficient and accepted security procedures, ignored significant warning available in the literature and chose to institute token authentication procedures as its security to protect against unauthorized transfers from customer's accounts.

187. CDA instructed Sovereign's representative that CDA had not made any wire transfers and Sovereign was not to honor any requested wire transfers on June 26, 2012.

188. Despite CDA's instruction to Sovereign's representative that CDA had not made any wire transfers and Sovereign was not to honor any requested wire transfers on June 26, 2012, Sovereign approved wire transfers of funds.

189. The Federal Financial Institutions Examination Council ("FFIEC") is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.

190. On June 28, 2011, the FFIEC issued a supplement to the *Authentication in an Internet Banking Environment* guidance, issued in October 2005. The purpose of the supplement was to reinforce the risk-management framework described in the original guidance and update the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment.

191. The FFIEC supplemental guidance provided that "the continued growth of electronic banking and greater sophistication of the associated threats have increased risks for financial institutions and their customers. Customers and financial institutions have experienced substantial losses from online account takeovers. Effective security is essential for financial institutions to safeguard customer information, reduce fraud stemming from the theft of sensitive customer information, and promote the legal enforceability of financial institutions' electronic agreements and transactions."

192. The supplement stressed the need for performing risk assessments, implementing effective strategies for mitigating identified risks, and raising customer awareness of potential risks, but did not endorse any specific technology for doing so.

193. The FFIEC directed examiners to formally assess financial institutions under the enhanced expectations outlined in the supplement beginning in January 2012.

194. The FFIEC guidance of June 2011, defined "Layered Security Programs" as "characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control…"

195. The FFIEC guidance provided, in part, that "layered security can substantially strengthen the overall security of Internet-based services and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses…"

196. Regulations and guidelines, specifically addressing financial institutions' responsibilities to protect customer information and prevent identity theft, are contained in the Interagency Final Regulation and Guidelines on Identity Theft Red Flags, 12 CFR parts 41, 222, 334, 571, and 717 and in the Interagency Guidelines Establishing Information Security Standards, 12 CFR parts 30, 208, 225, 364, and 570, Appendix B.

197. The FFIEC guidance provided, in part, that "financial institutions should implement a layered approach to security for high-risk Internet-based systems."

198. The FFIEC guidance provided, in part, that "effective controls that may be included in a layered security program include, but are not limited to:

a. fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;

b. the use of dual customer authorization through different access devices;

c. the use of out-of-band verification for transactions;

d. the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;

e. enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);

f. internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;

g. policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;

h. enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and

i. enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk."

199. The FFIEC guidance provided, in part, that "…an institution's layered security program will contain the following two elements, at a minimum.

a. Detect and Respond to Suspicious Activity

b. Layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:

i. initial login and authentication of customers requesting access to the institution's electronic banking system; and

ii. initiation of electronic transactions involving the transfer of funds to other parties."

200. The FFIEC guidance concluded, in part, that "[b]ased upon the incidents the Agencies have reviewed, manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior."

201. The FFIEC guidance additionally provided that, "for business accounts, layered security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. These enhanced controls should exceed the controls applicable to routine business customer users. For example, a preventive control could include requiring an additional authentication routine or a transaction verification routine prior to final implementation of the access or application changes. An example of a detective control could include a transaction verification notice immediately following implementation of the submitted access or

application changes. As discussed in the Appendix, out-of-band authentication, verification, or alerting can be effective controls. Based upon the incidents the Agencies have reviewed, enhanced controls over administrative access and functions can effectively reduce money transfer fraud."

202. The FFIEC guidance provided, in part, that "[t]ransaction monitoring/anomaly detection software…in use for a number of years…[by]… the credit card industry detects and blocks fraudulent credit card transactions, systems are now available to monitor online banking activity for suspicious funds transfers. They can stop a suspicious ACH/wire transfer before completion and alert the institution and/or the customer so that the transfer can be further authenticated or dropped. Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring/anomaly detection could have assisted in preventing many fraudulent money transfers as they were clearly out of the ordinary when compared with the customer's established patterns of behavior."

203. For anomalous transactions, the FFIEC recommend requiring "out-of-band" authentication or verification, which means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. However, out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised.

204. The FFIEC has stated, "[f]or business customers, the out-of-band authentication or verification should be provided by someone other than the person who first initiated the transaction and can be combined with other

administrative controls…and…can be an effective control to reduce fraudulent funds transfers."

205. The FFIEC, in its June 2011 guidance, concluded, in part, that "the Agencies agree with security experts who believe that institutions should no longer rely on one form of customer authentication. A one dimensional customer authentication program is simply not robust enough to provide the level of security that customers expect and that protects institutions from financial and reputation risk."

206. Sovereign Bank's web site for business accounts indicates a requirement of a Personal Identification Number for wire transfers initiated over the phone, in stating:

> "Wire Transfer
>
> Sovereign's Wire Transfer service is the most expedient method for transferring funds between your Sovereign business account and other bank accounts.
>
> It can be used for domestic or international transactions in which no cash or check exchange is involved, but the account balance is directly debited electronically and the funds are transferred to another account in real time. Sovereign offers multiple delivery channels to quickly, reliably, and securely initiate an immediate domestic or international transfer through our Wire Room, using your assigned Personal Identification Number, over the telephone or through Business Online Banking with BillPay."

207. Sovereign Bank failed to offer its customer participation in its "Automated alerts" program, which would have included "Wire Alerts—notify you whenever a wire transfer is sent or received." Summary information would have been sent via email to the customer.

208. Sovereign Bank represented to its customer that it "will never send an unsecured email requesting your User ID, Password, debit card number or any other sensitive information."

209. Despite the Bank's understanding that it should not be requesting "sensitive information" from its customer in an "unsecured email", the Bank, through its agent, forwarded all of the customer account information, including account numbers and balances, to the cybercriminal in an unsecure email.

210. The Bank's representations and advice to its customers concerning security warned, "**Same old con man, new ride**—Con men and women have been around since the beginning of human history, and the computer and Internet just represent new tools for their scams. In this category fall the infamous Nigerian scammers, crooks who trick you into unauthorized bank transfers and perform other forms of fraud. The difference between this and other types of cybercrime is that the crooks form a sort of relationship with the victim, fooling them into parting with their money." In this case, the Bank foolishly parted with its customer's money.

211. On August 21, 2012, in its response to CDA's counsel's demand to restore its account balance, Denise A. Gaudet, Deputy General Counsel for Sovereign Bank acknowledged that, "…I can tell you, however, that the bank did attempt a

call-back to confirm these wires. Unfortunately, the telephone number used for the call-back was not a valid telephone number for Chestnut Dental Associates, P.C. ("CDA").

**COUNT I**

**(LIABILITY PURSUANT TO M.G.L. c. 106, UCC § 4A-201, ET. SEQ.)**

212. Plaintiff incorporates the allegations contained in paragraphs 1-211 as set forth in this Complaint above as if fully set forth herein.

213. As described in this Complaint, on June 25 and 26 and July 3 and 10, Sovereign Bank received fraudulent wire transfer instructions from the perpetrators.

214. These wire transfer instructions were not authorized by CDA, nor was CDA bound by these wire transfer instruction pursuant to the law of agency.

215. These wire transfer instructions were not effective as the orders of CDA pursuant to § 4A-202 of the Uniform Commercial Code ("UCC"), codified at M.G.L.A. 106 § 4A-202

216. CDA and Sovereign did not enter into an agreement that allowed for variation from the established security procedure, which was verification of the wire transfer authorization by a call from Sovereign to CDA's office and confirmation by Jonathan Chason, D.M.D. or Jack Hertzberg, D.M.D.

217. To the extent that CDA and Sovereign did enter into an agreement that allowed for variation from the established security procedure, which was verification of the wire transfer authorization by a call from Sovereign to CDA's

office and confirmation by Jonathan Chason, D.M.D. or Jack Hertzberg, D.M.D., the steps taken by Sovereign to verify the authenticity of the fraudulent wire transfer authorizations issued on June 25, 26 and July 3 and 10 were outside the scope of and were not part of any such agreed-upon security procedure.

218. To the extent that CDA and Sovereign did enter into an agreement that allowed for variation from the established security procedure, which was verification of the wire transfer authorization by a call from Sovereign to CDA's office and confirmation by Jonathan Chason, D.M.D. or Jack Hertzberg, D.M.D., such security procedure was not a commercially reasonable method of providing security against fraudulent wire transfer authorizations for at least the following reasons:

a. Sovereign did not detect and prevent the fraudulent wire transfers even though the perpetrator:

i. Submitted the fraudulent transfer requests at a time when the account holder had never wired funds, and in fact the account holder had only completed a single annual wire transfer for its December Bonus Payroll;

ii. were the first international wire transfers for the account holder;

iii. were the only wire transfers not paid to their payroll company's account;

iv. listed as customer name an individual stockholder, not the name of the corporation, which was the account holder;

v. failed to list the customer's address;

vi. listed a prior address of Dr. Hertzberg, which he had not lived in for twelve years;

vii. listed a loan account number and not a deposit account;

viii. provided the return call phone number which was not the account holder's number;

ix. NEVER appeared at the bank for authorization;

x. Requested account information, including account numbers and balances, which the bank provided to the perpetrator in unsecured emails in multiple exchanges;

xi. deviated from the account holder's historic one time per year use to their payroll account;

xii. deviated from the account holder's loan application;

xiii. provided invoice numbers which failed to match the fraudulent wire transfer authorization;

219. To the extent that CDA and Sovereign did enter into an agreement that allowed for variation from the established security procedure, which was verification of the wire transfer authorization by a call from Sovereign to CDA's office and confirmation by Jonathan Chason, D.M.D. or Jack Hertzberg, D.M.D., such security procedure was not a commercially reasonable method of providing security against fraudulent wire transfer authorizations for at least the following reasons:

a. Sovereign failed to:

i. Utilize reasonable security testing procedure;

ii. Apply reasonable security testing procedures to each wire transfer transaction individually;

iii. Offer to send emails to CDA alerting it to unusual transactions;

iv. Reasonably verify the account holder's identity and authority;

v. as CDA had only sent one wire annually in the past ten plus years prior to June 25, 2012 and thus transaction verification with respect to CDA would not have been a burden to Sovereign or CDA;

vi. detect the fraud despite the fraudulent wire transfers of funds being sent to numerous individual accounts to which CDA had never before transferred funds;

vii. properly train and prevent its employee from sending account holder information via an unsecure email, which included account numbers and balances.

viii. have fraud monitoring programs in place or preventative security features to perform fraud scoring or fraud screening measurements on transactions to detect unusual activity.

220. To the extent that CDA and Sovereign did enter into an agreement that the authenticity of wire transfer authorizations would be verified pursuant to a security procedure, Sovereign did not approve the wire transfer authorizations in good faith and in compliance with that security procedure.

221. Sovereign breached this duty by failing to employ proper security procedures to prevent the fraudulent transfer of CDA's funds as described above.

222. Sovereign's breach of duty has caused significant economic harm to CDA as described above.

223. Sovereign's breach of duty was undertaken with malice, or is so outrageous that malice can be implied from its actions.

WHEREFORE, Plaintiff CDA respectfully requests that the Court enter Judgment against Defendant Sovereign Bank for damages in an amount to be determined at trial, together with interest, costs, attorney's fees and such other further relief as the Court deems just and appropriate.

## COUNT II

## (NEGLIGENCE)

224. Plaintiff incorporates the allegations contained in paragraphs 1-223 as set forth in this Complaint above as if fully set forth herein.

225. Sovereign had a duty to employ proper security procedures to ensure that parties other than CDA would not be able to effect transfers of funds from CDA's accounts by fraudulent means.

226. Sovereign breached this duty by failing to employ proper security procedures to prevent the fraudulent transfer of CDA's funds as described above.

227. Sovereign's breach of duty has caused significant economic harm to CDA as described above.

228. Sovereign's breach of duty was undertaken with malice, or is so outrageous that malice can be implied from its actions.

WHEREFORE, Plaintiff CDA respectfully requests that the Court enter Judgment against Defendant Sovereign Bank for damages in an amount to be determined at trial, together with interest, costs, attorney's fees and such other further relief as the Court deems just and appropriate.

## COUNT III

## (BREACH OF CONTRACT)

229. Plaintiff incorporates the allegations contained in paragraphs 1-228 as set forth in this Complaint above as if fully set forth herein.

230. By accepting CDA's deposits and the fees paid by CDA for banking services, Sovereign entered into an implied contract with CDA whereby Sovereign agreed that it would safeguard CDA's deposits against fraudulent transfers.

231. By failing to employ proper security procedures to prevent fraudulent transfer of CDA's funds as described above, Sovereign breached the aforementioned implied contract.

232. As a direct and proximate result of the breach of contract by Sovereign, CDA has suffered and will continue to suffer significant financial damages.

WHEREFORE, Plaintiff CDA respectfully requests that the Court enter Judgment against Defendant Sovereign Bank for damages in an amount to be determined at trial, together with interest, costs, attorney's fees and such other further relief as the Court deems just and appropriate.

## COUNT IV

## (BREACH OF FIDUCIARY DUTY)

233. Plaintiff incorporates the allegations contained in paragraphs 1-232 as set forth in this Complaint above as if fully set forth herein.

234. As CDA's bank, Sovereign owed fiduciary duties to CDA that included without limitation, the duties to safeguard CDA's funds and employ proper

security procedures to ensure that parties other than CDA would not be able to effect transfer of funds from CDA's accounts by fraudulent means.

235. By failing to safeguard CDA's funds and employ proper security procedures to prevent the fraudulent transfer of CDA's funds as described above, Sovereign breached its fiduciary duties to CDA.

236. Sovereign's breach of fiduciary duty has caused significant economic harm to CDA as described above.

237. Sovereign's breach of fiduciary duties was undertaken with malice, or is so outrageous that malice can be implied from its actions.

WHEREFORE, Plaintiff CDA respectfully requests that the Court enter Judgment against Defendant Sovereign Bank for damages in an amount to be determined at trial, together with interest, costs, attorney's fees and such other further relief as the Court deems just and appropriate.

## COUNT V

## (BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING)

238. Plaintiff incorporates the allegations contained in paragraphs 1-237 as set forth in this Complaint above as if fully set forth herein.

239. Implied in the relationships between the Plaintiff and the Defendant is the obligation on the part of the Defendant to act in good faith and deal fairly with the Plaintiffs.

240. Defendant's conduct in failing to comply with accepted security practices, protecting the Plaintiff's property and refusing to restore the Plaintiff's account balances and making it whole constituted a breach of the implied covenant of good faith and fair dealing.

241. As a direct and proximate result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff suffered actual damages in an amount to be determined by the Court.

WHEREFORE, Plaintiff CDA requests that this Court enter judgment in favor of the Plaintiff and award damages in an amount that is just and proper, with costs and reasonable attorneys' fees, and such other and further relief as the Court deems just and proper.

## COUNT VI

**(Massachusetts General Law C. 93A, § 11)**

242. Plaintiff incorporates the allegations contained in paragraphs 1-241 as set forth in this Complaint above as if fully set forth herein.

243. Plaintiff and Defendant are each persons engaged in the conduct of trade and commerce within the meaning of G.L. c. 93A.

244. Defendant's acts and conduct, as described in the preceding paragraphs, constitute unfair and deceptive acts and practices in the conduct of trade or commerce in violation of G.L. c. 93A, §§ 2 and 11. The Defendant's wrongful acts occurred primarily and substantially within the Commonwealth and were conducted intentionally, knowingly and willfully.

245. As a consequence of the Defendant's wrongful acts and conduct, Plaintiff has suffered the loss of both money and property, and the Defendant has been unjustly enriched.

WHEREFORE, Plaintiff requests that this Court enter judgment in favor of Plaintiff and award double or treble the amount of actual damages, in an amount that is just and proper, with costs and reasonable attorneys' fees pursuant to G.L. c. 93A, § 11, and such other and further relief as the Court deems just and proper.

**PLAINTIFFS DEMAND TRIAL BY JURY ON ALL OF THE FOREGOING COUNTS**

RESPECTFULLY SUBMITTED,
CHESTNUT DENTAL ASSOCIATES, P.C.
By its attorneys,
PABIAN & RUSSELL LLP,
By:

*/S/ Marc Kornitsky*

Marc D. Kornitsky
BBO# 564552
265 Franklin Street
Boston, MA 02110
(978) 532-5143 (direct)
(978) 532-3789 (fax)
mkornitsky@pabianrussell.com

By:

*/S/ Jay Pabian*

Jay M. Pabian
BBO# 386600
265 Franklin Street
Boston, MA 02110
(617) 951-3100 (office)
(617) 951-9929 (fax)
jpabian@pabianrussell.com

Dated: October 30, 2012